Notes on problem 15
Kevin Hughes

n is and odd integer, not a square. Define

$$H' = \{x = a + b\sqrt{D} \in (\mathbb{Z}/n[\sqrt{D}])^* | x^n = a + bD^{(n-1)/2}\sqrt{D}\}$$

Note that $\sqrt{D} \in H'$.

When is H' a group?

Claim H' is a group if and only if $D^n \equiv D$ (n is a fermat pseudoprime to base D).
Proof ($\Rightarrow$) Since H' is a group and $\sqrt{D} \in H'$, $(\sqrt{D})^2 = D \in H'$. And thus, $D^n \equiv D$.
($\Leftarrow$) Assume that $D^n \equiv D$, then for $x_1 = a_1 + b_1\sqrt{D}, x_2 = a_2 + b_2\sqrt{D} \in H'$:

$$x_1x_2 = (a_1 + b_1\sqrt{D})(a_2 + b_2\sqrt{D})$$

$$= (a_1a_2 + b_1b_2D) + (a_1b_2 + a_2b_1)\sqrt{D}$$

and,

$$(x_1x_2)^n = (x_1)^n(x_2)^n$$
$$= (a_1 + b_1D^{(n-1)/2}\sqrt{D})(a_2 + b_2D^{(n-1)/2}\sqrt{D})$$
$$= (a_1a_2 + b_1b_2D^n) + (a_1b_2 + a_2b_1)D^{(n-1)/2}\sqrt{D}$$
$$\equiv (a_1a_2 + b_1b_2D) + (a_1b_2 + a_2b_1)D^{(n-1)/2}\sqrt{D}$$

therefore, $x_1x_2 \in H'$. And of course $1 \in H'$ and H' is finite, so H' is a group.

When is H' a subgroup of $(\mathbb{Z}/n[\sqrt{D}])^*$?

Note that H' is a subgroup of $(\mathbb{Z}/n[\sqrt{D}])^*$ only if $\sqrt{D} \in (\mathbb{Z}/n[\sqrt{D}])^*$.

Claim $D \in (\mathbb{Z}/n)^*$ if and only if $\sqrt{D} \in (\mathbb{Z}/n[\sqrt{D}])^*$.
Proof If $D \in (\mathbb{Z}/n)^*$ then $(\sqrt{D})^{-1} = \sqrt{D} \cdot D^{-1}$ and D^{-1} exists, so $\sqrt{D} \in (\mathbb{Z}/n[\sqrt{D}])^*$. Conversely, if $D \notin (\mathbb{Z}/n)^*$, then D^{-1} does not exist and therefore, $\sqrt{D}^1$ does not exist and thus $\sqrt{D} \notin (\mathbb{Z}/n[\sqrt{D}])^*$.

So H' is a subgroup of $(\mathbb{Z}/n[\sqrt{D}])^*$ only if $D \in (\mathbb{Z}/n)^*$.

Claim If n is prime, then $H' = (\mathbb{Z}/n[\sqrt{D}])^*$.
Proof Let n be a prime, then $D^n \equiv D$. And if $x = a + b\sqrt{D} \in (\mathbb{Z}/n[\sqrt{D}])^*$, then

$$x^n = a^n + (b\sqrt{D})^n$$

$$\equiv a + bD^{(n-1)/2}\sqrt{D}$$

This implies that for all $(\mathbb{Z}/n[\sqrt{D}])^* \subseteq H'$ and we already know that $H' \subseteq (\mathbb{Z}/n[\sqrt{D}])^*$. Therefore $H' = (\mathbb{Z}/n[\sqrt{D}])^*$.